STMIK Amik Riau

SATIN – Sains dan Teknologi Informasi

journal homepage : http://jurnal.stmik-amik-riau.ac.id

Pengembangan Sistem Keamanan Jaringan Menggunakan Rumusan Snort Rule (Hids) untuk Mendeteksi Serangan Nmap

Pandu Pratama Putra
Jurusan Teknik Informatika, STMIK Amik Riau
pandupratamaputra@stmik-amik-riau.ac.id

Abstrak

Keamanan jaringan menjadi hal yang penting untuk semua industri dan perusahaan untuk menjaga keamanan jaringan, data dan informasi yang berada didalamnnya. Host-based Intrusion Detection System (HIDS) yang dimana Aktivitas sebuah host jaringan individual akan dipantau apakah terjadi sebuah percobaan serangan atau penyusupan ke dalamnya atau tidak. snort merupakan bagian dari IDS dan merupakan sebuah perangkat lunak open source. Snort mampu melakukan analisa real time alert, dimana mekanisme pemasukan alert dapat berupa user syslog, file atau melalui database. Sehingga dapat mendeteksi serangan pada jaringan komputer lebih awal. Metode yang digunakan yaitu penelitian lapangan (field research), penelitian perpustakaan (library research), serta penelitan laboratorium (laboratory research). Maka dari itu dapat diharapkan sistim keamanan yang lebih kuat terhadap serangan.

Kata Kunci : Keamanan Jaringan, HIDS, Snort Rule

1. Pendahuluan

1.1 Latar Belakang

Perkembangan teknologi khususnya di bidang *Networking* membuat bermacam – macam fitur, teknologi dan *tools* berkembang secara cepat dan baik. Komputer dan teknologi jaringan menyediakan kemudahan untuk masyarakat khususnya internet. Melalui internet, informasi dapat ditemukan secara beragam oleh siapapun dan kapanpun, tetapi dalam waktu yang sama internet tidak hanya memberikan efek positif untuk jaringan namun ancaman permasalahan kemanan jaringan yang penting dan lebih sangat serius. Perkembangan terhadap ancaman-ancaman *attacker*, *Intruder* atau *cracker* semakin meluas. Bahkan, banyak yang memilih untuk mengembangkan perlindungan jaringan daripada hal lain. Menurut *Information Week Research Priorities Survey Of 200 IT Executives*, menyebutkan bahwa Beberapa IT memilih sekitar 78% Responden untuk pengembangan keamanan jaringan dibandingkan, menaikkan *bandwidth*, *management* jaringan terpusat atau alokasi *bandwidth* per aplikasi atau *user*.

Keamanan jaringan menjadi hal yang penting untuk semua industri dan perusahaan untuk menjaga keamanan jaringan, data dan informasi yang berada didalamnnya. Berdasarkan perlindungan keamanan data/informasi dalam suatu jaringan, umumnya semua teori keamanan berbasis data dibuat dan diaplikasikan untuk mengamankan suatu jaringan tertentu. Teori keamanan data menggunakan teori kriptografi, riset, integritas dan ketersediaan data, strategi keamanan, dan lainnya. Metode - metode keamanan jaringan yang sudah muncul seperti menggunakan IDS (*intrusion detection system*), IPS (*Intrusion Prevention System*), *Firewall*, *network security based of knowledge* untuk menghambat terjadinya penyerangan atau penyusupan. Cara-cara yang digunakan bervariasi tergantung kebutuhan pengguna. *Intrusion Detection System* (IDS) adalah salah satu sistem yang dirancang sebagai bagian dari sistem keamanan jaringan komputer yang penting perananya dalam menjaga intergritas dan validitas serta

memastikan ketersediaan layanan bagi seluruh pengguna.

Untuk melakukan analisa untuk mengetahui serangan jaringan komputer mengunakan *Host-based Intrusion Detection System* (HIDS) yang dimana Aktivitas sebuah *host* jaringan individual akan dipantau apakah terjadi sebuah percobaan serangan atau penyusupan ke dalamnya atau tidak.

1.2 Perumusan Masalah

Berdasarkan latar belakang masalah di atas, maka dapat dijelaskan rumusan masalah dari studi kasus tentang analisa Vulneribilitas *Host* pada keamanan jaringan komputer sebagai berikut :

1. Bagaimana *Snort Rule Host-based Intrusion Detection System* (HIDS) memantau jaringan komputer ?
2. Bagaimana cara mendeteksi serangan di lingkungan *internal* ?
3. Bagaimana *Host-based Intrusion Detection System* (HIDS) dapat menentukan serangan apa yang terjadi pada jaringan ?
4. Bagaimana kinerja analisa pada keamanan jaringan komputer menggunakan *Host-based intrusion detection system* ?

1.3 Tujuan Penelitian

Adapun tujuan penelitiaan yang akan dicapai adalah sebagai berikut :

1. Mengetahui serangan apa yang terjadi pada sebuah jaringan komputer.
2. Menganalisa serangan apa yang terjadi pada jaringan komputer.
3. Menganalisa jaringan komputer yang diserang.

2. Landasan Teori

Salah satu prinsip dasar jaringan computer adalah proses pengiriman data atau informasi dari pengirim ke penerima melalui media komunikasi tertentu. Dari prinsip dasar tersebut maka tujuan dibangunnya suatu jaringan komputer adalah untuk membawa data atau informasi dari si pengirim ke penerima secara cepat tanpa adanya kesalahan. (Sulistianto & Suharno, 2012)

Intranet mulai dibicarakan pada pertengahan tahun 1955 oleh beberapa penjual produk jaringan yang mengacu pada kebutuhan informasi berbentuk web dalam suatu organisasi (kantor). Keuntungan yang mengacu pada kebutuhan informasi dalam membangun system jaringan komputer antara lain :

1. Dapat saling berbagi (sharing) penggunaan peralatan yang ada, seperti harddisk, printer, modem, dll tanpa memindahkan peralatan tersebut kepada yang membutuhkan. Sehingga mengemat waktu dan biaya pembelian hardware.
2. Dapat saling berbagi (sharing) penggunaan file atau data pada server atau workstation sehingga menghemat waktu.
3. Aplikasi dapat dipakai bersama-sama (multiuser).
4. Pengontrolan para pemakai atau pemakaian data secara terpusat oleh orangorang tertentu.
5. Sistem backup yang mudah karena menejemen tersentralisai. Sehingga tidak tergantung pada orang yang menyimpan data. (Santoso & Sumirat, 2012)

2.1 Keamanan Jaringan Komputer

Keamanan jaringan didefinisikan sebagai sebuah perlindungan dari sumber daya terhadap upaya penyingkapan, modifikasi, utilisasi, pelarangan dan perusakan oleh *person* yang tidak diijinkan. Bisa juga diartikan sebagai suatu perlindungan yang diusahakan oleh suatu sistem informasi dalam rangka mencapai sasaran hasil yang bisa diterapkan atau memelihara integritas, kerahasiaan dan ketersediaan sistem informasi sumber daya. Sumber daya informasi meliputi perangkat keras, perangkat lunak, data dan informasi.

Masalah keamanan menjadi salah satu perhatian pada jaringan nirkabel karena resiko keamanan semakin bertambah seiring semakin populernya jaringan nirkabel. Berikut beberapa ancaman yang umum ditemui pada jaringan nirkabel:

- MAC Spoofing
  Penyerang berusaha mendapatkan koneksi ke dalam jaringan dengan mengambil alamat NIC dari suatu perangkat komputer pada jaringan tersebut
- ARP Spoofing
  Penyerang menangkap penyebaran paket ARP dari *access point* dan kemudian mengirimkan balasan ARP fiktif sehingga informasi perangkat dari penyerang akan terpetakan ke dalam tabel ARP untuk kemudian mendapatkan hak akses kedalam jaringan. (Junior, Harianto, & Alexander, 2009)

Kebijakan keamanan (*security policy*) adalah suatu *set* aturan yang menetapkan hal-hal apa saja yang diperbolehkan dan apa saja yang dilarang terhadap penggunaan atau pemanfaatan akses pada sebuah sistem selama operasi normal. Penetapan kebijakan keamanan (*security policy)* ini hendaknya ditulis secara *detail* dan jelas. Tugas dan penetapan *security policy* biasanya merupakan keputusan politis dari manajemen perusahaan.(Amin, 2012) “Analisis Vurnerabilitas Host pada Keamanan Jaringan Komputer di Pt.

Sumeks Tivi Palembang (PALTV) Menggunakan Router Berbasis Unix

Analisis ancaman adalah sebuah proses *audit* di mana semua kemungkinan penyerangan terhadap sistem diidentifikasi secara cermat. Sebuah catatan yang memuat semua daftar kemungkinan penyalahgunaan dan gangguan terhadap sistem hendaknya dibuat sebagai basis peringatan.

Gambar 1. *Rule Security Policy*

Penerapan kebijakan aturan-aturan *security policy* hendaknya dilakukan secara sistematis dengan terlebih dahulu melakukan sebuah analisis awal, baik itu analisis terhadap instalasi fisik maupun *logic*, meliputi: *audit* dan penyeimbangan antara ongkos proteksi sistem dengan resiko-resiko yang ditimbulkan, barulah kemudian dilakukan implementasi mekanisme–mekanisme keamanan yang telah dirancang tersebut, sebagai contoh mekanisme *access control* yang menerangkan objek-objek mana saja yang diizinkan untuk diakses publik dan mana yang tidak.

Secara umum, terdapat 3 hal dalam konsep keamanan jaringan, yakni:

1. Resiko atau tingkat bahaya (*risk*) yaitu: Menyatakan besarnya kemungkinan gangguan yang muncul terhadap jaringan.
2. Ancaman (*threat*) yaitu : Menyatakan kemungkinan gangguan yang muncul terhadap jaringan.
3. Kerapuhan sistem (*vulnerability*) yaitu: Menyatakan kelemahan- kelemahan pada sistem yang memungkinkan terjadinya gangguan.

Keamanan jaringan komputer itu sendiri menyangkut 3 elemen dasar yakni :

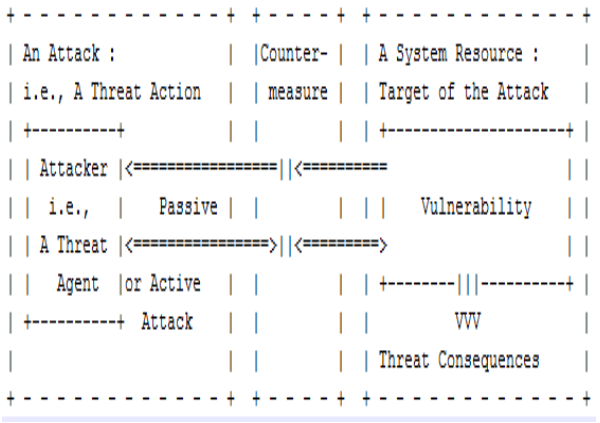
1. Keamanan jaringan *(network security)* : Upaya pengamanan atas jalur / media pengiriman data.
2. Keamanan aplikasi *(application security)* : Upaya pengamanan atas aplikasi-aplikasi dan layanan yang tersedia, contohnya DBMS.
3. Keamanan komputer *(computer security)* : Upaya pengamanan atas komputer yang digunakan untuk memakai aplikasi, termasuk di dalamnya adalah sistem operasi.

Masalah keamanan jaringan komputer secara umum dibagi menjadi empat kategori yang saling berkaitan:

1. *Secrecy/confidentiality*: Informasi yang dikirim melalui jaringan komputer harus dijaga sedemikian rupa kerahasiaannya sehingga tidak dapat diketahui oleh pihak yang tidak berhak mengetahui informasi tersebut.
2. *Authentication*: Identifikasi terhadap pihak-pihak yang sedang melakukan komunikasi melalui jaringan harus dapat dilakukan. Pihak yang berkomunikasi melalui jaringan harus dapat memastikan bahwa pihak lain yang diajak berkomunikasi adalah benar-benar pihak yang dikehendaki.
3. *Nonrepudiation*: Pembuktian korespondensi antara pihak yang mengirimkan informasi dengan informasi yang dikirimkan juga perlu dilakukan dalam komunikasi melalui jaringan komputer. Dengan pembuktian tersebut, identitas pengirim informasi dapat dipastikan dan penyangkalan pihak tersebut atas informasi yang telah dikirimnya tidak dapat dilakukan.
4. *Integrity control*: Informasi yang diterima oleh pihak penerima harus sama dengan informasi yang dikirim oleh pengirim. Informasi yang telah mengalami perubahan dalam proses pengiriman, misalnya diubah oleh pihak lain, harus dapat diketahui oleh pihak penerima.

2.2 Konsep Dasar Vulnerabilitas

Sebuah vulnerabilitas adalah suatu poin kelemahan dimana suatu sistem rentan terhadap serangan. Sebuah ancaman (*threats*) adalah suatu hal yang berbahaya bagi keberlangsungan system(Amin, 2012). Ada tiga kata kunci yang timbul dan saling berkaitan apabila kita mendiskusikan mengenai isu-isu daripada kemanan komputer, yaitu: vulnerabilitas, ancaman (*threats*), dan tindakan pencegahan (*countermeasures*) seperti diilustrasikan pada gambar 2 dibawah.



Gambar 2. Diagram Vulnerabilitas

Bahaya tersebut dapat berupa manusia (*a syste cracker or a spy*), suatu peralatan yang rusak, atau sebuah kejadian seperti kebakaran dan banjir, yang mungkin dapat mengeksploitasi kerentanan suatu sistem. Semakin banyak vulnerabilitas dan ancaman

yang dapat terjadi didalam suatu sistem, sudah seharusnya semakin tinggi pula kesadaran kita untuk dapat memproteksi sistem dan informasi yang berada didalamnya. Sebuah teknik untuk melindungi suatu sistem dinamakan dengan tindakan pencegahan (*countermeasures*) (Amin, 2012).

3. Metode Penelitian

Dengan memperhatikan cakupan kegiatan penelitian dari aspek kurun waktu pelaksanaan kegiatan penelitian, cara memperoleh informasi yang dibutuhkan, tujuan penelitian dan merujuk lebih lanjut kepada referensi serta ahli jaringan komputer, sehingga penelitian ini bersifat deskriptif, karena tujuan dari penelitian ini adalah bagaimana meminimalisir vulnerabilitas keamanan jaringan komputer.

3.1 Kerangka Kerja Penelitian

1. Identifikasi Masalah

Pada penelitian ini merupakan tahap awal dalam melakukan penelitian dengan mengidentifikasi masalah kita bisa mengetahui masalah apa yang akan kita bahas dalam penelitian ini.

2. Menentukan Tujuan Penelitian

Berdasarkan identifikasi masalah yang telah dibuat pada tahap sebelumnya, maka tahap penentuan tujuan berguna untuk memperjelas kerangka tentang apa saja yang menjadi sasaran dari penelitian ini. Pada tahap ini ditentukan tujuan dari penelitian ini adalah bagaimana merancang dan membangun sistem keamanan jaringan komputer sehingga menghasilkan *host* yang lebih aman dari serangan dan ancaman pada sistem keamanan *host* CV. Hayati Padang.

3. Literatur

Melalui studi literatur, dipelajari teori - teori yang berhubungan dengan jaringan komputer, serangan terhadap jaringan komputer, vulnerabilitas *host* keamanan jaringan komputer dan tentang penggunaan metode *(Intrusion Detection Sistem) Snort Rule* untuk pengujian keamanan jaringan komputer sehingga didapatkan sebuah kesimpulan. Sumbernya berupa buku, jurnal, maupun situs internet yang berhubungan dengan keamanan jaringan komputer dan metode - metode yang berhubungan *(Intrusion Detection Sistem) Snort Rule.*

4. Pengumpulan Data

Pengumpulan data dan informasi pada tahap ini dilakukan untuk megetahui, mendapatkan data dan informasi yang nantinya akan mendukung penelitian ini, dalam pengumpulan data, terdapat beberapa metode yang digunakan yaitu penelitian lapangan (*field research*), penelitian perpustakaan (*library research*), serta penelitan laboratorium (*laboratory research*).

5. Analisis Sistem

Analisis sistem dapat didefinisikan sebagai penguraian dari suatu sistem yang utuh. Dalam melakukan analisis masalah penelitian melakukan beberapa cara dan metode diantaranya Metode Diskriptif. Pada metode ini data yang ada dikumpulkan, disusun, dikelompokkan, dianalisis sehingga diperoleh beberapa gambaran yang jelas pada masalah penelitian tersebut. Metode Komperatif, pada metode ini analisis dilakukan dengan cara membandingkan teori dan praktek sehingga diperoleh gambaran yang jelas tentang persamaan dan perbedaan diantara keduanya.

6. Perancangan Sistem

Tahap ini akan dilakukan proses perancangan dan metode analisis terhadap vulnerabilitas keamanan jaringan komputer serta metode yang digunakan dalam mengatasinya. Pada tahap ini melakukan konfigurasi pada *Snort* yang merupakan gambaran dari solusi yang akan dihasilkan, dengan konfigurasi dan *rule* nya dapat menghasilkan output yang diinginkan yaitu *host* (komputer) aman dari serangan atau penyusup lainnya.

7. Analisa dan Pembangunan Sistem

Tahap ini membahas tentang pembangunan dari sistem dengan langkah-langkah yang telah dilakukan pada identifikasi masalah dan menganalisis kelemahan dari *host* yang dituju, dan melakukan pengujian dan perbaikan sistem sehingga sesuai kreteria yang diinginkan.

8. Pengujian Sistim

Tahap berikutnya setelah perancangan dan pembangunan sistem adalah pengujian sistem. Hal ini dilakukan untuk melihat sejauh mana metode *IDS Snort Rule* ini mampu memecahkan permasalahan. Pengujian dilakukan dengan berbagai macam serangan (serangan bersifat internal) yang dilakukan pada *host* sasaran. Hasilnya kemudian dievaluasi apakah sudah sesuai dengan hasil yang dicapai dalam keamanan jaringan komputer.

4. Analisa dan Pembangunan Sistem

4.1 Identifikasi Masalah

Keamanan jaringan komputer merupakan hal penting untuk ditingkatkan, apalagi terkoneksi dengan *internet* yang dapat diakses dari berbagai negara / area dan *user*. Dengan hal itu banyak sekali tindakan kejahatan yang dilakukan oleh orang yang tidak bertanggung jawab terhadap sistem dengan berbagai serangan terhadap sistem.

4.2 Analisis Sistem

Pada dasarnya penelitian yang dilakukan pada tahapan analisis ini ada dua bagian, yaitu tahap pengumpulan data dan analisis yang secara garis besar untuk memperoleh pengertian dari permasalahan -

permasalahan, dan pertimbangan-pertimbangan yang mengarah kepada pengembangan sistem. Memperkirakan kendala - kendala yang akan dihadapi dalam pengembangan sistem tersebut dan menentukan solusi - solusi *alternative.*

4.3 Analisa Sistem Yang sedang berjalan

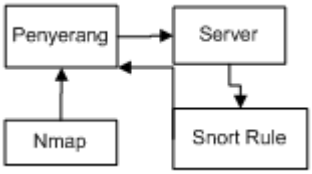
Merupakan suatu kegiatan untuk mengetahui sistem yang dipakai sebelum adanya sistem yang baru dalam proses menyediakan layanan keamanan pada *network*. Analisis dilakukan dalam upaya untuk mengetahui kelemahan yang ada pada sistem yang digunakan. Pada saat ini sistem masih menggunakan konfigurasi yang masih ada vulnerabilitas sehingga dapat menimbulkan ancaman terhadap sistem.

4.4 Permasalahan yang Dihadapi

Berdasarkan peninjauan langsung pada CV. Hayati Padang permasalahan yang dihadapi adalah masih terdapat vulnerabilitas (kelemahan) pada sistem dan belum adanya penambahan *source* yang menyebabkan sistem tidak dapat mendeteksi adanya serangan pada sistem seperti serangan *Denial of Service* (DoS) yang bentuk serangan-serangan terhadap *server*, salah satu penyerang yang melakukan kiriman paket dalam jumlah besar terhadap *server*, sehingga menyebabkan *load* CPU meningkat dan *traffic* pun menjadi padat. Kejadian seperti di atas dapat menimbulkan *threats (*ancaman) bagi sistem CV. Hayati Padang. Hal ini menjadikan pemikiran untuk menjadikan sistem yang lebih *secur*e.

4.5 Alur Serangan

Dalam alur serangan ini akan diceritakan bagaimana terjadinya serangan. Pada Gambar 3 dapat di lihat alur serangan.

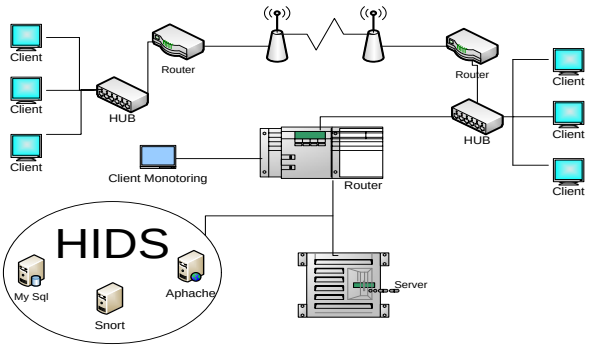


Gambar 3. Alur Serangan

Dari gambar 3 maka akan di jabarkan bagaimana langkah – langkah terjadinya serangan dan bagaimana snort rule mendeteksi serangan Nmap. Pertama sekali hal yang di lakukan penyerang adalah dengan melakukan scan IP dengan Nmap. Lalu langkah selanjudnya penyerang akan mendapatkan port yang terbuka pada *server*, setelah penyerang mendapatkan informasi port yang terbuka, maka snort tersebut akan melakukan deteksi terhadap penyerang yang melakukan scan port terhadap *server*. Snort akan memberitahu kepada administrator bahwa terdapat serang yang berupa scanning port *server*, sehingga administrator dapat melakukan tindakan pencegahan terlebih dahulu.

4.6 Alternatif Pemecahan Masalah

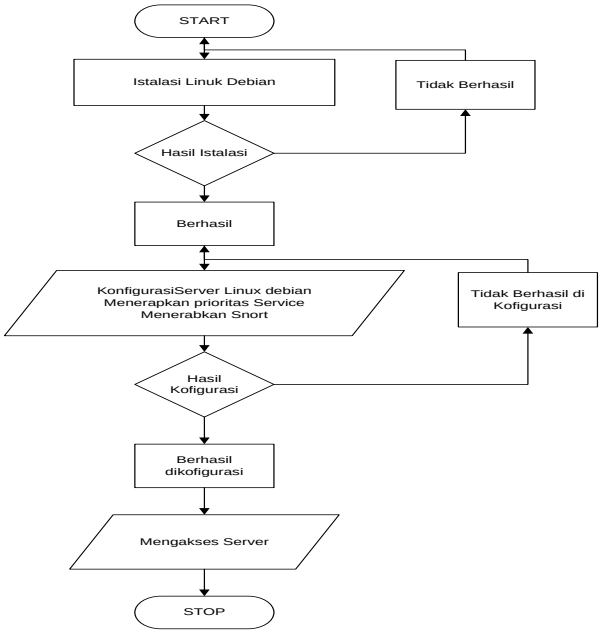
Dalam proses peningkatan keamanan jaringan komputer dan ancaman dari penyerang *network* CV. Hayati Padang maka diperlukan suatu sistem berbasiskan teknologi keamanan jaringan komputer. Sistem keamaan jaringan komputer menggunakan metode IDS. Berikut gambar 4perancangan yang baru :



Gambar 4. Rangkaian yang baru

4.7 Desain Proses

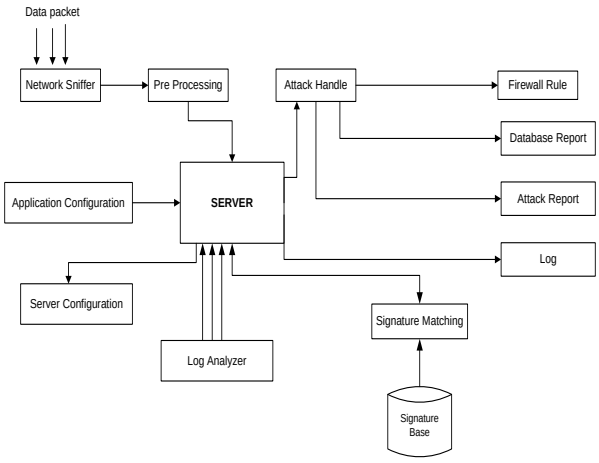
Setelah tahapan analisa kebutuhan dan perancangan, maka akan diuraikan desain proses dalam membangun PC *Server*. Berikut ini alur proses dan *state diagram* yang digunakan dalam penelitian ini :



Gambar 5. Model Alur proses Flowchart

4.8 Diagram *Core Engine Intrussion Detection System*

Core Engine bertindak sebagai bagian dari *Intrusion Detection System* yang berhadapan langsung dengan berbagai serangan. Layaknya program atau *server* di lingkungan *Unix / Linux, core engine* memiliki banyak proses yang bekerja secara bersama namun dapat saling berkomunikasi satu sama lain. Diagram sistem dapat dilihat pada gambar 6 :



Gambar 6. *Diagram Core Engine Intrussion Detection System*

5. Implementasi dan Pengujian

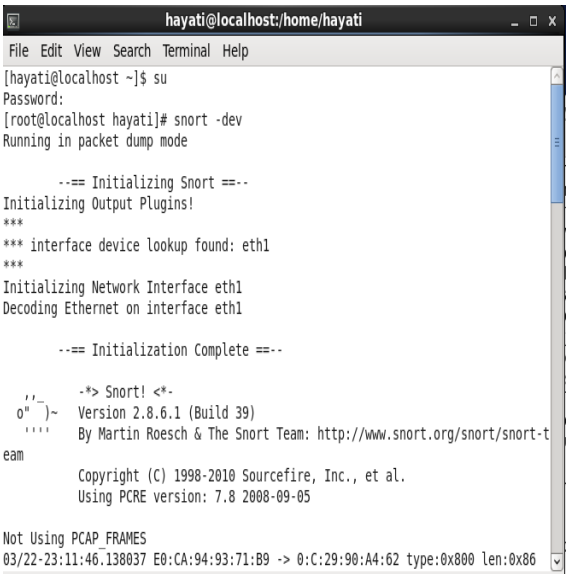
5.1 Skenario Tes

Skenario tes menjelaskan bagaimana sistem dijalankan. *Admin login* ke dalam *server* setelah itu melakukan konfigurasi terhadap *server*, mulai dari konfigurasi *IP Address,* installasi *web server*, *snort* beserta *rule*-nya.Setelah semuanya diinstal, semua *service* yang dibutuhkan dijalankan dengan *command* pada *terminal Centos.* Jika semua benar, maka *server* akan memberikan komentar *"ok",* dan sistem siap digunakan.

Pada sistem ini menggunakan *client monitoring* untuk melakukan *monitoring* aktivitas *user* terhadap sistem / *server.* Pada *cline monitoring* ini juga menggunakan *tools snort* beserta *rule-rulenya* untuk menghasilkan *log* ke dalam *file client monitoring.*

5.2 Implementasi *Snort*

Tools snort yang sudah di install pada *server*, untuk menggunakannya dengan menggunakan *command* seperti : "snort –dev", maka akan tampil Gambar 7 yang menjelaskan keterangan dari informasi *tools* yang digunakan dan keterangan dari sistem seperti *IP Address, port* yang terkoneksi dengan *server* atau yang melakukan *ping* terhadap *server.*



Gambar 7. Informasi *Snort* pada *Server*

5.3 Implementasi *Client Monitoring*

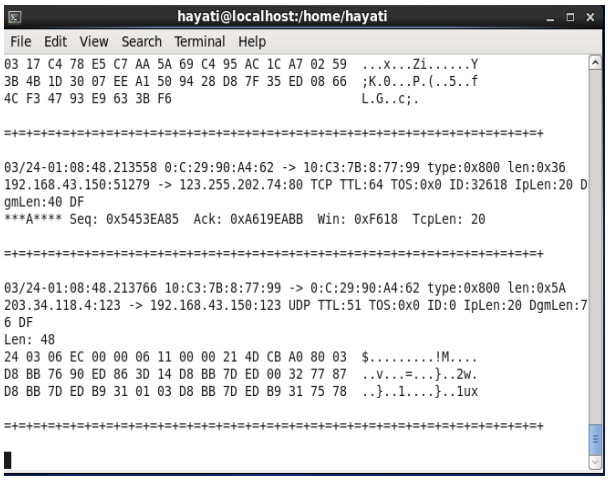
Client monitoring fungsinya selain peranannya sebagai *client*, juga sebagai *monitoring* aktivitas yang dilakukan oleh *client* terhadap sistem (*server).* Pada *client monitoring* ini juga diinstal *tolls snort, rule* dan *libarary* yang dibutuhkan.

a. Monitoring dari *client*
   Sebagaimana yang sudah dijelaskan di atas, *monitoring* dilakukan oleh *client* dimana fungsinya memantau aktivitas terhadap sistem. *Client* disini menggunakan sistem operasi *Windows 7,* dengan *command:* **c:\Snort\bin>snort -dev -i 1.** Dengan mengetikkan *command* tersebut maka akan muncul informasi mengenai aktivitas terhadap sistem, seperti komputer yang mengakses *server* dengan identitas berupa *IP Address*, seperti pada Gambar 8

Gambar 8. Keterangan Aktivitas *Client*

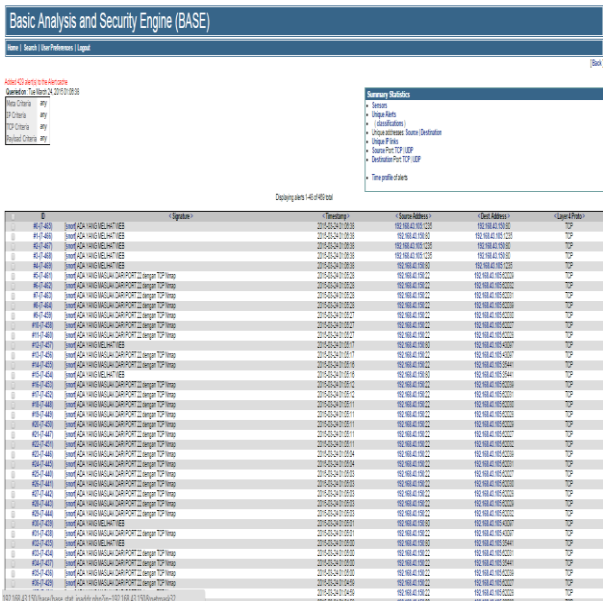
5.4 Pengujian Terhadap Sistem yang Sudah *Secure*

Pengujian ini dilakukan terhadap sistem yang sudah di proteksi oleh sistem, yaitu dengan menggunakan metode IDS *Snort*. Sewaktu *intruder* melakukan serangan terhadap sistem seperti melakukan scan dengan Nmap, sistem dapat mendeteksi aktivitas tersebut. Sistem akan menampilkan aktifitas intruder dalam bentuk pemberitahuan ke *server* dan *file .log* yang di simpan dalam *file C:\Snort\log,command* yang di ketikkan adalah : "snort –dev seperti terlihat dalam gambar 9.



Gambar 9. Aktivitas Sistem

Bagi *intruder* yang mencoba masuk melewati *port* 22 dan akan terdeteksi oleh sistem , seperti terlihat pada Gambar 10**.**



Gambar 10. Aktifitas Client dan Penyerang

5.5 Hasil Pengujian

Berdasarkan hasil pengujian di atas *snort rule* dapat memberitahukan aktifitas serangan terhadap *server*, baik pengujian dilakukan dengan serangan *Nmap*.

Secara umum hasil pengujian pada sistem dengan metode IDS *Snort rule* dapat di lihat dari tabel 1.

Tabel 1. Hasil Pengujian

No	Indikator	Hasil
1.	Serangan seperti Nmap	Diketahui oleh *Snort Rule*
2.	*Log* Aktivitas	Adanya *record* ke dalam log *client monitoring*

6. Simpulan

Hasil pengujian implementasi *Snort Rule* sebagai bagian dari HIDS telah berhasil mendeteksi serangan *DoS*, sehingga dapat di simpulkan bahwa rumusan *Snort Rule* yang di bangun telah bekerja dengan baik. Implementasi *Snort Rule* mampu mendeteksi serangan *DoS* maka dapat disimpulkan, bahwa rumusan *Snort Rule* yang dibangun bisa membantu tugas *admin* untuk mengamankan sitem jaringan.

Referensi

Amin, Z. (2012). Analisis Vulnerabilitas Host Pada Keamanan Jaringan Komputer Di Pt . Sumeks Tivi Palembang (Paltv) Menggunakan Router Berbasis Unix. *Analisis Vulnerabilitas Host Pada Keamanan Jaringan Komputer Di Pt. Sumeks Tivi Palembang (Paltv) Menggunakan Router Berbasis Unix*, *2*(3), 189–199.

Junior, A. N. S., Harianto, A., & Alexander. (2009). Perancangan dan Implementasi Intrusion Detection System pada Jaringan Nirkabel BINUS University. *BINUS University Jakarta*.

Santoso, D. H., & Sumirat, E. W. (2012). Pembangunan Jaringan Local Area Network Smp Negeri 2 Sumberlawang. *Seruni FTI UNSA 2012 Volume 1*, *1*, 19–23.

Sulistianto, D. A., & Suharno, P. (2012). Pembangunan Jaringan Komputer Commanditaire Vennootschap (CV) Dino Mandiri Karanganyar. *Seruni FTI UNSA 2012 Volume 1*, *1*(Cv), 1–8.

https://www.snort.org/downloads/community/opensource.tar.gz

https://www.snort.org/downloads/snortplus/snort_extra-1.0.0-a3-cmake.tar.gz